UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION, Plaintiff, v. SOLARWINDS CORP. and TIMOTHY G. BROWN, Defendants.	)	Judge Paul A. Engelmayer Civil Action No. 23-cv-9518-PAE

MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANTS' MOTION TO EXCLUDE THE TESTIMONY OF MARK G. GRAFF

Table of Contents

INTRODUCTION 1

BACKGROUND 2

I. SolarWinds' Security Statement Misrepresentations 2

II. Mark Graff's Expert Report and Opinions 3

ARGUMENT 6

I. Legal Standard 6

II. Mr. Graff's Opinions are Directly Relevant to the Issues in Dispute 7

III. Mr. Graff's Expert Opinions are Based on Decades of Cybersecurity Experience 10

A. Mr. Graff Employed Technical Cybersecurity Expertise in His Report 10

B. Defendants Point to No Relevant Evidence Mr. Graff Failed to Analyze 12

C. Mr. Graff Analyzed and Explained Highly Technical Documents 14

IV. Mr. Graff's Opinions are Based on A Reliable Methodology Using His Decades of Cybersecurity Experience 17

A. Defendants Improperly Challenge Mr. Graff's Conclusions Regarding SolarWinds' Failures to Consistently Follow Its Stated Cybersecurity Practices 17

B. Defendants' Attempts to Challenge the Substance of Mr. Graff's Opinions are Wholly Improper in a Daubert Motion 20

V. Mr. Graff is not Opining on Scienter 23

CONCLUSION 25

Table of Authorities

Cases

In re Aluminum Warehousing Antitrust Litig.,
336 F.R.D. 5 (S.D.N.Y. 2020) 18, 20

BanxCorp v. Costco Wholesale Corp.,
978 F. Supp. 2d 280 (S.D.N.Y. 2013).....17, 18

Berman v. Mobil Shipping & Transp. Co.,
2019 WL 1510941 (S.D.N.Y. Mar. 27, 2019) 9, 13

Bernstein v. Cengage Learning, Inc.,
2023 WL 6303424 (S.D.N.Y. June 9, 2023) 7

Better Holdco, Inc. v. Beeline Loans, Inc.,
666 F. Supp. 3d 328 (S.D.N.Y. 2023).....11

Boykin v. W. Exp., Inc.,
2015 WL 539423 (S.D.N.Y. Feb. 6, 2015).....13, 14

Capri Sun GmbH v. Am. Beverage Corp.,
595 F. Supp. 3d 83 (S.D.N.Y. 2022).....7, 14

Caruso Mgmt. Co. Ltd. v. Int'l Council of Shopping Centers,
403 F. Supp. 3d 191 (S.D.N.Y. 2019).....11

CFTC v. Wilson,
2016 WL 7229056 (S.D.N.Y. Sept. 30, 2016).....25

Chill v. Calamos Advisors LLC,
417 F. Supp. 3d 208 (S.D.N.Y. 2019).....13

City of Providence v. Bats Glob. Markets, Inc.,
2022 WL 902402 (S.D.N.Y. Mar. 28, 2022) 9

Daubert v. Merrell Dow Pharm., Inc.,
509 U.S. 579 (1993).....6, 8, 21

In re Digital Music Antitrust Litig.,
321 F.R.D. 64 (S.D.N.Y. 2017) 7

Doe v. City of New York,
2024 WL 1134568 (S.D.N.Y. Mar. 15, 2024) 8

In re Elysium Health-ChromaDex Litig.,
2022 WL 421135 (S.D.N.Y. Feb. 11, 2022).....9

In re Fosamax Prods. Liab. Litig.,
924 F. Supp. 2d 477 (S.D.N.Y. 2013).....23

Hnot v. Willis Grp. Holdings Ltd.,
2007 WL 1599154 (S.D.N.Y. June 1, 2007).....9

In re Joint E. & S. Dist. Asbestos Litig.,
52 F.3d 1124 (2d Cir. 1995).....21

Kumho Tire Co. v. Carmichael,
526 U.S. 137 (1999).....7

In re LIBOR-Based Fin. Instruments Antitrust Litig.,
299 F. Supp. 3d 430 (S.D.N.Y. 2018).....21, 22

Lickteig v. Cerberus Cap. Mgmt., L.P.,
589 F. Supp. 3d 302 (S.D.N.Y. 2022).....7

LinkCo, Inc. v. Fujitsu Ltd.,
2002 WL 1585551 (S.D.N.Y. July 16, 2002).....17

LVL XIII Brands, Inc. v. Louis Vuitton Malletier S.A.,
209 F. Supp. 3d 612 (S.D.N.Y. 2016).....20

LVL XIII Brands, Inc. v. Louis Vuitton Malletier S.A.,
720 F. App'x 24 (2d Cir. 2017).....20

In re Lyman Good Dietary Supplements Litig.,
2019 WL 5682880 (S.D.N.Y. Oct. 31, 2019).....9

Malletier v. Dooney & Bourke, Inc.,
525 F. Supp. 2d 558 (S.D.N.Y. 2007).....9

In re Mirena IUD Prods. Liab. Litig.,
169 F. Supp. 3d 396 (S.D.N.Y. 2016).....10

Nimely v. City of New York,
414 F.3d 381 (2d Cir. 2005).....6

Novartis Pharma AG v. Incyte Corp.,
2024 WL 3608338 (S.D.N.Y. July 29, 2024).....16

In re Pfizer Inc. Sec. Litig.,
819 F.3d 642 (2d Cir. 2016).....9

Powers v. Mem'l Sloan Kettering Cancer Ctr.,
2022 WL 874846 (S.D.N.Y. Mar. 24, 2022).....11

PRCM Advisers LLC v. Two Harbors Investment Corp.,
2025 WL 1276513 (S.D.N.Y. May 2, 2025).....7

Schoolcraft v. City of New York,
2015 WL 6444620 (S.D.N.Y. Oct. 23, 2015).....8

Scott v. Chipotle Mexican Grill, Inc.,
315 F.R.D. 33, 45 (S.D.N.Y. 2016).....16

SEC v. AT&T, Inc.,
626 F. Supp. 3d 703 (S.D.N.Y. 2022).....2

SEC v. Lek Sec. Corp.,
370 F. Supp. 3d 384 (S.D.N.Y. 2019).....20

SEC v. Ripple Labs, Inc.,
2023 WL 5670711 (S.D.N.Y. Mar. 6, 2023).....23

SEC v. Tourre,
950 F. Supp. 2d 666 (S.D.N.Y. 2013).....6

Ultra Recs., LLC v. Ultra Int'l Music Publ'g, LLC,
2024 WL 4663011 (S.D.N.Y. Nov. 4, 2024).....7

United States ex rel. Bassan v. Omnicare, Inc.,
2025 WL 66443 (S.D.N.Y. Jan. 10, 2025).....18

United States v. Guo,
2024 WL 2262706 (S.D.N.Y. May 17, 2024).....9

United States v. Mejia,
545 F.3d 179 (2d Cir. 2008).....16

United States v. Napout,
963 F.3d 163 (2d Cir. 2020).....6

United States v. Onumonu,
967 F.2d 782 (2d Cir. 1992).....12

United States v. Zhong,
26 F.4th 536 (2d Cir. 2022) 12

U.S. Bank Nat. Ass'n v. PHL Variable Life Ins. Co.,
112 F. Supp. 3d 122 (S.D.N.Y. 2015).....13

In re Vivendi, S.A. Sec. Litig.,
838 F.3d 223 (2d Cir. 2016).....9

Rules

Fed. R. Evid. 401 8

Fed. R. Evid. 702 .....1, 6, 10, 12, 14

Fed. R. Evid. 703 16

Pursuant to the Court's March 14, 2025, Scheduling Order (ECF No. 163) and Federal Rule of Evidence 702, Plaintiff Securities and Exchange Commission ("SEC") respectfully submits this memorandum of law in opposition to Defendants' Motion to Exclude the Testimony of Mark G. Graff (ECF No. 183).

INTRODUCTION

Defendants' goal in filing a *Daubert* challenge to Mr. Graff is clear. In the first instance, they want the Court to grant them summary judgment based on a one-sided view of the evidence that ignores the significance of cybersecurity failures that SolarWinds' own employees contemporaneously documented. Alternatively, if their summary judgment motion is denied, they want the Court to prevent the jury from benefiting from the decades of cybersecurity expertise and experience that Mr. Graff brings to this case. Defendants' efforts, however, must fail. Their motion is premised on mischaracterizations of Mr. Graff's expert opinions and a misunderstanding of the applicable law governing expert testimony. Rather than address the actual opinions set forth in Mr. Graff's thorough and comprehensive reports, Defendants instead attack their own mischaracterizations of Mr. Graff's reports.

Each of the independent arguments Defendants advance for excluding Mr. Graff are without merit. First, Mr. Graff's expert opinions about inconsistencies between SolarWinds' public descriptions of their cybersecurity practices in the Security Statement and SolarWinds' private internal assessments of those practices are unquestionably relevant and "fit" the SEC's allegations. Second, Mr. Graff's opinions, which are based on a technical analysis of relevant SolarWinds' documents using decades of experience in the cybersecurity field and recognized industry guidelines and standards, undoubtedly reflects the use of cybersecurity expertise. Third, Defendants' challenges to the substance of Mr. Graff's conclusions are wholly improper in a

Daubert motion and instead should be raised in cross-examination at trial. And finally, Mr. Graff offers no opinions regarding Defendants' state of mind or scienter. Instead, he offers opinions about what SolarWinds' serious cybersecurity lapses should have indicated to company leadership—a perfectly acceptable topic for expert testimony.

Defendants' motion should be denied for all these reasons, as explained in detail below.[1]

BACKGROUND

I. SolarWinds' Security Statement Misrepresentations

As alleged in the Amended Complaint, SolarWinds and Brown materially misrepresented the company's cybersecurity practices in the "Security Statement" made publicly available on SolarWinds' website. *See* AC, ¶¶ 7-8 (ECF No. 85). Specifically, the Security Statement was materially misleading in several aspects, including its representations about SolarWinds' access controls, its password practices, and the secure development lifecycle it purportedly used to develop software. *Id.* ¶ 7. The misleading Security Statement concealed from the public SolarWinds' internally known poor cybersecurity practices in each of these areas. *Id.* ¶ 8.

Numerous internal documents prepared by Brown and others reflect internal assessments that sharply contrasted with the robust cybersecurity practices depicted in the Security Statement. *See e.g., id.* ¶¶ 62-66. SolarWinds also omitted information from the Security Statement necessary to make the information included within it not misleading. *Id.* ¶ 72. The known cybersecurity failures, risks, and incidents, "so affected SolarWinds' cybersecurity posture that

[1] The Court could also deny Defendants' motion without prejudice because, as demonstrated in the SEC's opposition to Defendants' motion for summary judgment filed today, the SEC can defeat summary judgment simply by relying on lay evidence. *See SEC v. AT&T, Inc.*, 626 F. Supp. 3d 703, 741 & n. 43 (S.D.N.Y. 2022) (Engelmayer, J.).

SolarWinds needed to, at a minimum, disclose their collective effect, especially in light of the Security Statement's positive portrayal of SolarWinds' cybersecurity practices." *Id.* ¶ 73.

II. Mark Graff's Expert Report and Opinions

The SEC has proffered Mark Graff to testify as a cybersecurity expert and to compare the internal cybersecurity assessments Brown and other SolarWinds employees made contemporaneously with the representations made by Brown and the company in the Security Statement. Mr. Graff submitted an initial expert report on October 25, 2024. Exhibit 1 to Graff Decl. ("Graff Rep."). He then submitted a rebuttal report on January 24, 2025, in response to the critiques offered by Defendants' putative expert Dr. Rattray. Exhibit 2 to Graff Decl. ("Graff Rebuttal").

Mr. Graff holds a Bachelor of Science degree in Computer Science. He has over 40 years' experience as a computer programmer, technologist, and cybersecurity executive. Graff Rep., ¶ 1. He has "designed cyber defenses, managed the groups that operated those defenses, written security plans and security policies, and overseen the response to many cybersecurity incidents." *Id*. He operates a cybersecurity consulting company, Tellagraff LLC, through which he provides consulting services to businesses and the government, provides expert testimony, and teaches college courses regarding cybersecurity and secure software development. *Id.* ¶¶ 1, 5. As a consultant, he works with clients to evaluate and remediate cybersecurity threats and risks. *Id.* ¶ 2.

Previously, Mr. Graff served as the Chief Information Security Officer ("CISO") of NASDAQ OMX from 2012 to 2015[2] and as the Chief Cyber Security Officer / Chief Cyber

[2] Defendant's state in their motion that Mr. Graff left this position "nearly 10 years ago." Def. Mot. at 2. However, despite their expert Gregory Rattray misrepresenting his credentials in his report and curriculum vitae, the truth is he left his position as CISO at JPMorgan in June 2015,

Security Strategist at Lawrence Livermore National Laboratory from 2003 to 2012. *Id.* at A-1. At NASDAQ, he led a team that secured NASDAQ's worldwide operations against cyber-attacks by foreign countries, criminal organizations, and other hostile entities. *Id.* ¶ 3. He also directed NASDAQ's global security policy, implemented their cybersecurity awareness training, and developed secure software applications. *Id*. At Lawrence Livermore, Mr. Graff managed the organization's cybersecurity program, where he conducted numerous cybersecurity research projects and risk analyses in the interest of national security. *Id*. Lawrence Livermore focuses on national security concerns such as nuclear proliferation, terrorism and energy security, and helping manage the nation's nuclear stockpile. *See https://www.llnl.gov/about* (last visited June 3, 2025).

Prior to these positions, Mr. Graff spent twenty years in various cybersecurity roles at different companies. Graff Rep. ¶ 4. In those roles he worked on incident prevention and response, threat analysis, and risk evaluation. *Id*. He also served as Chairman of the Forum of Incident Response and Security Teams ("FIRST"), an international association of enterprise cyber-defense teams. *Id*. Mr. Graff has also co-authored three books about security and software. *Id.* ¶ 6. One of his books has been used at dozens of universities to teach how to design and build secure software-based systems. *Id*. Additionally, Mr. Graff has testified before Congress on matters of internet and software security. *Id*. ¶ 7.

Here, Mr. Graff performed a technical comparison between the state of cybersecurity depicted in the SolarWinds Security Statement and SolarWinds' own internal assessments and communications regarding the state of cybersecurity in the 2017-2020 timeframe. *Id.* ¶ 17.

---

which is also nearly 10 years ago. *See* Mem. of Law in Support of Motion to Exclude Rattray at 19-21) (ECF No. 172).

Specifically, he focused his analysis on access control, user authentication, use of a secure development lifecycle, and adherence to the NIST Cybersecurity Framework. *Id*. In addition to considering SolarWinds' own internal analyses of the company's cybersecurity, Mr. Graff considered the testimony of SolarWinds employees taken in this matter. *Id.* ¶ 18.

Mr. Graff described in detail the methodology he followed in performing this technical comparison. *Id.* ¶ 45. First, he "reviewed the Security Statement, identifying those assertions within the ambit of the four areas which were sufficiently definite—that is, categorical—as to be either intrinsically verifiable or falsifiable." *Id.* Second, based on his many years of cybersecurity experience and his expertise in industry norms, he evaluated these practices against widely accepted industry norms. *Id*. Third, to conduct his comparison between what SolarWinds was saying internally about its state of cybersecurity and the public representations it was making in the Security Statement, Mr. Graff developed key words and terms to guide his team through searching the vast volume of documents produced by SolarWinds in this litigation. *Id*. These searches allowed him to focus on documents relating to the practices he was evaluating. *Id*. Additionally, he asked counsel for documents that, based on his experience, a company such as SolarWinds would possess and which he "considered to be relevant to evaluate SolarWinds' internal understanding of its cybersecurity posture." *Id*. Additionally, he reviewed investigative and deposition testimony from SolarWinds' employees regarding these issues. *Id*. Finally, employing his decades of cybersecurity experience, Mr. Graff evaluated SolarWinds' internal assessments and communications regarding the state of its cybersecurity against the public representations in the Security Statement. *Id*.

Based on his vast experience, his review of SolarWinds' own internal cybersecurity assessments and considering the language of the Security Statement, he concluded that the state

of cybersecurity in SolarWinds' internal assessments was inconsistent with the Security Statement in several areas. *Id.* ¶¶ 20, 48. Specifically, he concluded that "with respect to access control, user authentication, and secure development lifecycle processes, there were significant discrepancies between the cybersecurity practices SolarWinds claimed to be performing and the cybersecurity practices [he] observed from its internal documents." *Id.* ¶ 23.

ARGUMENT

I. Legal Standard

"The admissibility of expert testimony in the federal courts is governed principally by Rule 702 of the Federal Rules of Evidence." *United States v. Napout*, 963 F.3d 163, 187 (2d Cir. 2020) (quoting *Nimely v. City of New York*, 414 F.3d 381, 395 (2d Cir. 2005)). Federal Rule of Evidence 702 provides:

> A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if the proponent demonstrates to the court that it is more likely than not that:
>
> (a) the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;
>
> (b) the testimony is based on sufficient facts or data;
>
> (c) the testimony is the product of reliable principles and methods; and
>
> (d) the expert's opinion reflects a reliable application of the principles and methods to the facts of the case.

The trial court acts as a gatekeeper in determining whether to admit expert testimony. *Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579, 597 (1993). "To determine whether a proposed expert's testimony passes muster under Rule 702, this Court must inquire into: (1) the qualifications of the proposed expert; (2) whether each proposed opinion is based upon reliable data and reliable methodology; and (3) whether the proposed testimony would be helpful to the

trier of fact." *SEC v. Tourre*, 950 F. Supp. 2d 666, 674 (S.D.N.Y. 2013) (collecting cases); *accord Capri Sun GmbH v. Am. Beverage Corp.,* 595 F. Supp. 3d 83, 119 (S.D.N.Y. 2022) (Engelmayer, J.).

"In light of the liberal admissibility standards . . . exclusion of expert testimony is warranted only when the district court finds 'serious flaws in reasoning or methodology.'" *PRCM Advisers LLC v. Two Harbors Investment Corp.*, 2025 WL 1276513, at *4 (S.D.N.Y. May 2, 2025) (quoting *Lickteig v. Cerberus Cap. Mgmt., L.P.*, 589 F. Supp. 3d 302, 330 (S.D.N.Y. 2022)). "The federal courts employ a presumption of admissibility of expert evidence, such that the rejection of expert testimony is the exception rather than the rule." *Bernstein v. Cengage Learning, Inc.*, 2023 WL 6303424, at *9 (S.D.N.Y. June 9, 2023) (cleaned up). "When an expert's testimony rests upon good grounds, based on what is known, it should be tested by the adversary process—competing expert testimony and active cross-examination—rather than excluded from jurors' scrutiny for fear that they will not grasp its complexities or satisfactorily weigh its inadequacies." *Ultra Recs., LLC v. Ultra Int'l Music Publ'g, LLC*, 2024 WL 4663011, at *3 (S.D.N.Y. Nov. 4, 2024) (cleaned up). "If an expert's testimony lies within 'the range where experts might reasonably differ,' the jury, and not the trial court, should 'decide among the conflicting views of different experts.'" *In re Digital Music Antitrust Litig.*, 321 F.R.D. 64, 75 (S.D.N.Y. 2017) (quoting *Kumho Tire Co. v. Carmichael*, 526 U.S. 137, 153 (1999)).

II. Mr. Graff's Opinions are Directly Relevant to the Issues in Dispute.

Defendants advance a cramped and hyper-technical view of the concept of relevance to argue that Mr. Graff's opinions regarding SolarWinds' cybersecurity practices in relation to its Security Statement are somehow not relevant to this case—which is of course about that very subject. *See* Def. Mot. at 6-7. Yet, their view is not consistent with the law. *See Capri Sun GmbH*, 595 F. Supp. 3d at 140 (holding that party's argument "is wrong because it reads

Daubert's 'fit' requirement too narrowly.") (Engelmayer, J.). Instead, "expert testimony is relevant if it has 'any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence.'" *Doe v. City of New York*, 2024 WL 1134568, at *5 (S.D.N.Y. Mar. 15, 2024) (citation omitted); *see also* Fed. R. Evid. 401 ("Evidence is relevant if: (a) it has any tendency to make a fact more or less probable than it would be without the evidence; and (b) the fact is of consequence in determining the action."). "The Rules' basic standard of relevance is a liberal one." *See Schoolcraft v. City of New York,* 2015 WL 6444620, at *1 (S.D.N.Y. Oct. 23, 2015) (quoting *Daubert*, 509 U.S. at 587) (cleaned up).

As described above, Mr. Graff's assignment was to offer a technical comparison between the state of cybersecurity depicted in the SolarWinds Security Statement and SolarWinds' own internal assessments and communications regarding the state of cybersecurity in the relevant timeframe. The first paragraph of the SEC's Amended Complaint makes it clear that the opinions that Mr. Graff has offered in this regard easily satisfy the liberal relevance standard for expert testimony. The SEC alleges that "SolarWinds' public statements about its cybersecurity practices and risks painted a starkly different picture from internal discussions and assessments about the Company's cybersecurity policy violations, vulnerabilities, and cyberattacks." AC ¶ 1 (ECF No. 85). With respect to the Security Statement, the SEC alleged that "the misleading Security Statement concealed from the public the Company's known poor cybersecurity practices throughout the Relevant Period." *Id*. ¶ 8. The Amended Complaint further states that "in and around the same time that SolarWinds was making these materially misleading public statements, Brown and other SolarWinds employees knew that SolarWinds had serious

cybersecurity deficiencies. Internal emails, messages, and documents from the same period described many known material cybersecurity risks, control issues, and vulnerabilities." *Id*. ¶ 10.

Defendants claim that Mr. Graff's opinions must precisely trace the SEC's specific factual allegations and legal theories to be relevant to this matter. *See* Def. Mot. at 6-7. [3] Yet, courts have repeatedly rejected such arguments. *See In re Pfizer Inc. Sec. Litig.*, 819 F.3d 642, 661 (2d Cir. 2016) ("The dispositive question under Rule 702 is whether the testimony will assist the trier of fact not whether the testimony satisfies the plaintiff's burden on the ultimate issue at trial.") (cleaned up); *accord In re Vivendi, S.A. Sec. Litig.*, 838 F.3d 223, 260 (2d Cir. 2016); *Berman v. Mobil Shipping & Transp. Co.*, 2019 WL 1510941, at *10 (S.D.N.Y. Mar. 27, 2019); *United States v. Guo*, 2024 WL 2262706, at *3 n. 4 (S.D.N.Y. May 17, 2024). Defendants assert that Mr. Graff's opinions regarding the serious cybersecurity failures at SolarWinds do not themselves carry the SEC's burden. S*ee* Def. Mot. at 6-7. Not only is this an issue for a jury to decide, but even if it were accurate, "the expert testimony will neither confuse nor mislead the jury, but rather will help the jury to critically evaluate the plausibility of plaintiff['s] claims." *Hnot v. Willis Grp. Holdings Ltd.*, 2007 WL 1599154, at *3 (S.D.N.Y. June 1, 2007).

[3] The cases cited by SolarWinds in which courts have found expert testimony to not satisfy the liberal relevance requirement under Rule 702 are inapposite and involve experts discussing topics not even at issue in the particular cases. *See* Def. Mot. at 6-7 (citing *City of Providence v. Bats Glob. Markets, Inc.*, 2022 WL 902402, at *8–9 (S.D.N.Y. Mar. 28, 2022) (expert testimony not relevant because it did not examine the products at issue in the case); *In re Elysium Health-ChromaDex Litig.*, 2022 WL 421135, at *30 (S.D.N.Y. Feb. 11, 2022) (expert testimony irrelevant because it studied the synergistic effect between defendant's products and a co-enzyme that was not at issue in the case); *In re Lyman Good Dietary Supplements Litig.*, 2019 WL 5682880, at *5 (S.D.N.Y. Oct. 31, 2019) (portions of expert report irrelevant because it discussed the presence of chemicals not relevant to case); *Malletier v. Dooney & Bourke, Inc.*, 525 F. Supp. 2d 558, 573 (S.D.N.Y. 2007) (finding lack of fit between expert's report discussing lost sales since lost profits not at issue).

Defendants contend that "the theory the SEC has pled and must prove at trial is that SolarWinds suffered from pervasive cybersecurity failures with respect to the Subject Policies." *See* Def. Mot. at 6. Yet, even if they were correct about the SEC's burden[4], there can be no doubt that Mr. Graff's expert insights into the disconnect between the cybersecurity policies touted in the Security Statement and the reality Defendants discussed internally would "help the trier of fact to understand the evidence or to determine a fact in issue." Fed. R. Evid. 702.

III. Mr. Graff's Expert Opinions are Based on Decades of Cybersecurity Experience.

A. Mr. Graff Employed Technical Cybersecurity Expertise in His Report.

Defendants next claim that Mr. Graff's opinions, expressed in two robust and highly detailed reports with more than 500 footnoted citations, is "not based on any special expertise." Def. Mot. at 8. Defendants' claim is meritless. As described above, Mr. Graff has more than 40 years of professional cybersecurity experience and has written and taught extensively on the subject. It is that experience and knowledge that he has applied in offering his opinions in this matter. *See In re Mirena IUD Prods. Liab. Litig.*, 169 F. Supp. 3d 396, 413 (S.D.N.Y. 2016) ("In certain fields, experience is the predominant, if not sole, basis for a great deal of reliable expert testimony.") (quoting Fed. R. Evid. 702 advisory committee's note).

The employment of that vast experience in offering his opinions is evident throughout his reports. Take but a few examples:

- "Throughout my expert report, with respect to the four areas of focus in my assignment, I evaluated SolarWinds' cybersecurity posture described in the Security Statement based on my interpretation of the guidelines described by organizations such as NIST, as well as my first-hand experience with the implementation of well-accepted industry norms." Graff Rep. ¶ 44.
- "Below, I first describe examples where SolarWinds' internal documents indicate that the company's practices did not consistently conform to the Security Statement's assertions

[4] This issue is addressed fully in the SEC's opposition to Defendants' motion for summary judgment, filed today.

regarding access control (Sections IV.B.3.a-c). Then, in Section IV.B.3.d, I discuss in detail the implications and potential consequences of access control violations. As I will show, industry bodies such as NIST, ISO, SANS, CERT/CC, and CISA agree that a failure to follow commonly accepted access control practices, such as the principle of least privilege, can expose the organization to several types of risks, including, among others: (1) increased exposure to external attacks; (2) increased risk of insider threats; (3) increased difficulty with preventing, detecting, and responding to cyberattacks; and (4) other operational risks." *Id*. ¶ 60.

- "In this section, I first provide an overview of secure development lifecycles within the context of cybersecurity (Section IV.D.1). Second, I present potentially verifiable (or falsifiable) assertions SolarWinds made in its public Security Statement concerning developing software under a secure development lifecycle, including performing commonly accepted security tests (Section IV.D.2). Third, I interpret both the Security Statement and SolarWinds' internal documents describing the development of software under a secure development lifecycle in the context of the well-accepted industry norms that were available during the Relevant Period." *Id*. ¶ 138.

Defendants' primary argument in support of their claim that Mr. Graff's opinions are "not based on any special expertise" is that he took a different approach to conducting his analysis than did their expert Dr. Rattray. *See id*. at 8-9. Putting aside that Dr. Rattray's factual narrative should be excluded for the reasons set forth in the SEC's motion, Defendants offer no authority—only *ipse dixit*—for their contention that his approach is the correct one. *See Better Holdco, Inc. v. Beeline Loans, Inc.*, 666 F. Supp. 3d 328, 355 (S.D.N.Y. 2023) (denying *Daubert* motion that "essentially asks the Court to determine which of the two experts is more reliable."); *Powers v. Mem'l Sloan Kettering Cancer Ctr.*, 2022 WL 874846, at *5 (S.D.N.Y. Mar. 24, 2022) ("Where the parties present divergent expert testimony, it is the province of the jury to determine the credibility of the experts.") (cleaned up); *Caruso Mgmt. Co. Ltd. v. Int'l Council of Shopping Centers*, 403 F. Supp. 3d 191, 207 (S.D.N.Y. 2019) ("Ultimately, the credibility of the competing expert witnesses, and the persuasiveness of their opinions are all questions for the jury.") (cleaned up). Even if there were a single technique for assessing whether a company's public statements regarding cybersecurity were belied by its internal assessments, simply telling the Court "our expert's approach is the right one" is not how to prove that in a *Daubert* motion.

The Second Circuit, quoting the Advisory Committee Note to Rule 702, has recognized a commonsense test for evaluating the usefulness of expert testimony in a given case:

> There is no more certain test for determining when experts may be used than the common sense inquiry whether the untrained layman would be qualified to determine intelligently and to the best possible degree the particular issue without enlightenment from those having a specialized understanding of the subject involved in the dispute.

United States v. Onumonu, 967 F.2d 782, 788 (2d Cir. 1992) (quoting Fed. R. Evid. 702 advisory committee's note); *accord United States v. Zhong,* 26 F.4th 536, 555 (2d Cir. 2022).

Here, there can be no dispute that Mr. Graff's application of his decades of experience, knowledge, training, and service as a Chief Information Security Officer will help a lay jury determine whether SolarWinds' public statements regarding its cybersecurity practices matched its own internal assessments. Defendants offer no explanation as to how a lay jury would be expected to grapple with these complex technical issues without such assistance.

B. <u>Defendants Point to No Relevant Evidence Mr. Graff Failed to Analyze.</u>

Defendants next claim, without any support, that Mr. Graff "deliberately excluded" from his analysis relevant evidence. Def. Mot. at 9.[5] Yet, they point to no actual evidence that Mr.

[5] Defendants selectively and misleadingly quote a sentence from Mr. Graff's report in which he stated: "Even if I had found a large number of additional internal documents describing SolarWinds adhering to industry norms at times, these would not have changed my opinions." Def. Mot at 9 (quoting Graff Rep. ¶ 46). However, the three sentences that preceded that one in his report provide important and necessary context, showing that Defendants' characterization is incorrect:

> "Let me note that it was not necessary to review all SolarWinds internal documents related to a topic for me to reach a conclusion about whether the internal documents depicted a state of cybersecurity consistent with the assertions in the Security Statement. *I have found evidence of many flaws in SolarWinds' practices, and they are sufficient in the aggregate for me to conclude that SolarWinds did not consistently implement the practices described in several assertions in the Security Statement*. Reviewing additional documents would not

Graff should have considered but did not. *See Boykin v. W. Exp., Inc.*, 2015 WL 539423, at *6 (S.D.N.Y. Feb. 6, 2015) ("Defendant does not explain why any of the facts that [the expert] disregarded were crucial to the analysis."). To the extent Defendants are referring to the approximately 10,000 documents that they produced for the first time in conjunction with Dr. Rattray's report and which they described to the Court as "repetitive in nature" (*see* Order granting extension of expert discovery to allow for review of production) (ECF No. 155), Mr. Graff *did* consider those in conjunction with his rebuttal report. *See* Graff Rebuttal Report at Appendix A (listing materials considered). Moreover, as Mr. Graff explained in his rebuttal report with respect to these documents, "Dr. Rattray did a partial survey of policies and looked at some of the processes SolarWinds had during the Relevant Period. But he did *not* assess whether those policies and processes were enforced, or the extent to which the implementation of the policies was consistent with the Security Statement." *Id*. ¶ 19. In other words, Dr. Rattray simply pointed to the existence of documents to bolster his conclusions without evaluating their contents.

Furthermore, to the extent Defendants inaccurately contend that Mr. Graff ignored or failed to consider certain facts that they deem important, it is axiomatic that such challenges go to the weight of the testimony and are to be left for trial. *See Chill v. Calamos Advisors LLC*, 417 F. Supp. 3d 208, 246 (S.D.N.Y. 2019) ("As a general rule, the factual basis of an expert opinion goes to the *credibility* of the testimony, not the admissibility, and it is up to the opposing

---

> have changed my opinion because the flaws that I have found were so consequential in the aggregate that, from a cybersecurity perspective, they placed the company (and, in some cases, its customers) at profound cybersecurity risk and directly contradicted several assertions in the Security Statement."

Graff Rep. ¶ 46 (emphasis added).

party to examine the factual basis for the opinion in cross-examination.") (cleaned up); *accord Berman*, 2019 WL 1510941, at *11; *U.S. Bank Nat. Ass'n v. PHL Variable Life Ins. Co.*, 112 F. Supp. 3d 122, 134 (S.D.N.Y. 2015); *Boykin*, 2015 WL 539423, at *6. The same holds true for Defendants' allegation that Mr. Graff engaged in "cherry picking." *See Capri Sun GmbH*, 595 F. Supp. 3d at 135 (holding that critique that expert engaged in cherry-picking of facts is a "suitable subject[] for cross-examination but do[es] not warrant exclusion.").[6]

C. Mr. Graff Analyzed and Explained Highly Technical Documents.

Defendants next claim that "rather than analyzing such direct cybersecurity artifacts—which Mr. Graff might credibly claim to have special expertise in interpreting—Mr. Graff instead focuses on interpreting obscure language in emails and slide decks and purporting to divine whether the authors were stating something 'inconsistent' with the Security Statement." Def. Mot. at 9. However, this unsupported assertion is contradicted by the documents Mr. Graff analyzed, which contain technical, industry-specific language and concepts. Using his experience and expertise, Mr. Graff explained (1) the meaning of these technical concepts for a non-expert audience; (2) how the concepts in these documents relate to the practices laid out in the Security Statement; (3) how these practices relate to industry norms; and (4) what are the possible implications of not following such industry norms. As such, his expertise would "help the trier of fact to understand the evidence or to determine a fact in issue." Fed. R. Evid. 702.

Indeed, just a couple examples of Mr. Graff's detailed analyses of the evidence he reviewed belies Defendants' characterization of his efforts: *First,* in reviewing several internal email chains regarding an incident in which the password "solarwinds123" was inadvertently

[6] Defendants cannot be credibly suggesting that it is improper for an expert witness to be provided relevant documents by attorneys to consider. Defendants' expert Dr. Rattray, when asked how certain documents were selected, explained how Latham selected the documents for which he asked. See Rattray Depo. 204:10-22 (Exhibit A).

publicly disclosed, Mr. Graff explained technical concepts such as "hard-coded plaintext password" and what it means to "upload files to an FTP server." Graff Rep. ¶¶ 86-87, 126. He analyzed how this incident was relevant to the practices described in the Security Statement concerning password best practices and access control. *Id*. ¶ 77. He explained that storing a plaintext password in a configuration file violates commonly accepted industry norms. *Id*. ¶ 126 (citing OWASP guidance). He then described the potential serious ramifications of such a failure by explaining that "by publicly disclosing the credentials to SolarWinds' FTP site from which customers normally downloaded SolarWinds content, anyone on the internet could *upload* malicious software into this repository. SolarWinds' customers could then *download* these malicious files, while thinking that they were downloading legitimate SolarWinds materials." *Id*. ¶ 87.

Second, Mr. Graff reviewed several internal documents, including an email chain and risk acceptance forms, in which SolarWinds employees described engineers' inappropriate "SuperUser access" to production data. *Id*. ¶ 79. He explained technical concepts described in these internal documents. For example, Mr. Graff explained the difference between "read" access and "write" access, as well as the difference between "production" and "development" environments. *Id.* ¶¶ 81, 143. He compared the practices described in this email chain to the practices laid out in the Security Statement. Notably, he explained that (a) "[p]roviding unnecessary access to highly privileged accounts is inconsistent with the assertion that '[r]ole based access controls are implemented for access to information systems;'" (b) "[u]sing shared logins is inconsistent with the assertion that '[w]e require that authorized users be provisioned with unique account IDs;'" and (c) "[d]evelopers accessing the production dataset is inconsistent with the assertion that 'SolarWinds maintains separate development and production

environments." *Id.* ¶ 84. He then compared this practice to industry norms. *Id*. ¶ 105 ("Industry bodies, including NIST, ISO, SANS, CERT/CC, and CISA, agree that not following the principle of least privilege (and thus, not following commonly accepted access control practices), can expose the organization to several types of risks."); ¶ 143 ("As part of a secure software development methodology, it is widely accepted practice to provide security training to employees. It is also widely accepted practice to separate the development environment and the testing environment from the production environment."). Finally, Mr. Graff described the possible implications of this cybersecurity failure. *Id*. ¶ 83 (describing potential dangers of providing inappropriate read/write access); ¶¶ 151, 153 (describing potential dangers of a failure to separate the production environment from the development environment). [7]

Moreover, notwithstanding Defendants' complaint that Mr. Graff reviewed their "emails and slide decks" (Def. Mot. at 9) the law is clear that under Federal Rule of Evidence 703 an expert is permitted to form opinions based on documents by "applying his extensive experience and a reliable methodology" to those documents. *United States v. Mejia*, 545 F.3d 179, 197 (2d Cir. 2008) (citation omitted). Further, contrary to Defendants' claim that "*Daubert* and Rule 702 do not permit" experts to interpret technical communications and other such documents (*see* Def. Mot at 10), an expert "may offer commentary on documents in evidence if the expert's testimony relates to the context in which documents were created, defining any complex or specialized terminology, or drawing inferences that would not be apparent without the benefit of experience

[7] Ironically, Defendants further claim that Mr. Graff is simply narrating the SEC's view of the facts without applying expert analysis. *See* Def. Mot. at 9-11. However, while that accurately describes what Defendants' *own expert* did, as described in detail in the SEC's motion to exclude Dr. Rattray (ECF No. 172), that is not a fair description of Mr. Graff's reports. That is why the SEC's motion walked through example after example of Dr. Rattray simply narrating Defendants' preferred version of the facts. By contrast, Defendants do not give any examples of when Mr. Graff is supposedly engaged in narration.

or specialized knowledge." *Scott v. Chipotle Mexican Grill, Inc.*, 315 F.R.D. 33, 45 (S.D.N.Y. 2016) (cleaned up); *accord Novartis Pharma AG v. Incyte Corp.*, 2024 WL 3608338, at *20 (S.D.N.Y. July 29, 2024) (holding that expert's "reliable opinions may assist the factfinder in understanding the industry customs and practices applicable" to the complex matters at issue).[8]

IV. Mr. Graff's Opinions are Based on A Reliable Methodology Using His Decades of Cybersecurity Experience.

A. Defendants Improperly Challenge Mr. Graff's Conclusions Regarding SolarWinds' Failures to Consistently Follow Its Stated Cybersecurity Practices.

As described above, Mr. Graff performed a technical comparison between the state of cybersecurity depicted in the SolarWinds Security Statement and SolarWinds' own internal assessments and communications regarding the state of cybersecurity in the relevant timeframe. Graff Rep. ¶ 17. Mr. Graff described in detail the methodology he followed in performing this technical comparison. *Id.* ¶ 45. In short, he reviewed the Security Statement's assertions, applied his decades of cybersecurity expertise and experience to evaluate those assertions against industry norms, he then searched through the large volume of documents produced by SolarWinds for documents relating to the practices he was evaluating along with witness testimony on those subjects, and then evaluated SolarWinds' internal assessments and communications regarding its state of cybersecurity against the public representations in the Security Statement. *Id*. This is precisely what one would expect a cybersecurity expert to do in a case where the SEC has alleged that Defendants were saying one thing to the public through their

[8] One of the cases cited by Defendants, *LinkCo, Inc. v. Fujitsu Ltd*., 2002 WL 1585551, at *2 (S.D.N.Y. July 16, 2002) (cited at Def. Mot. at 10) involved the exclusion of an expert who simply restated deposition testimony, like Dr. Rattray did in this case. However, in a later case in which that same expert was allowed to testify, the court distinguished the case before it from *LinkCo* on the ground that now the expert was offering a technical interpretation of the evidence in the case. *BanxCorp v. Costco Wholesale Corp.*, 978 F. Supp. 2d 280, 322 (S.D.N.Y. 2013).

Security Statement while offering a much different assessment of the company's cybersecurity internally. Nowhere in their motion do Defendants offer any suggestion as to what different methodology a cybersecurity expert should use to compare a company's public statements with its internal ones.

Instead, Defendants spend half their brief attacking Mr. Graff's *conclusions* under the guise of challenging his *methodology*. *See e.g*, Def. Mot. at 13 ("The problem for Mr. Graff is that, if the first alternative is what he means, then he lapses into self-contradiction; and if the second alternative is what he means, then he lapses into irrelevance."). This Court has rejected misplaced challenges of this sort. *See In re Aluminum Warehousing Antitrust Litig*., 336 F.R.D. 5, 34 (S.D.N.Y. 2020) (observing that the defendant's "critique, although packaged in *Daubert* terms, is in substance a disagreement with [the expert's] conclusions.") (Engelmayer, J.). It is axiomatic that in conducting a *Daubert* analysis "the district court must focus on the principles and methodology employed by the expert, without regard to the conclusions the expert has reached or the district court's belief as to the correctness of those conclusions." *United States ex rel. Bassan v. Omnicare, Inc.*, 2025 WL 66443, at *2 (S.D.N.Y. Jan. 10, 2025) (citation omitted); *accord BanxCorp*, 978 F. Supp. 2d at 322 ("But these are objections to Webster's 'conclusions,' not to his 'methodology'—and thus Plaintiff has put forward exactly the type of argument the Supreme Court held irrelevant to admissibility in *Daubert.* Instead, objections to an expert's conclusions go to the weight of the evidence, not its admissibility.").

Rather than challenge the methodology that Mr. Graff used in forming his opinions—*i.e.*, comparing the technical assertions of the Security Statement regarding cybersecurity practices to internal technical discussions regarding those same practices—Defendants quibble with Mr. Graff's use of the word "consistently" in his *conclusion* that "SolarWinds failed to consistently

apply the cybersecurity practices described in the Security Statement." Def. Mot. at 12-13 (quoting Graff Rep. ¶ 48). Even if Defendants could transfigure Mr. Graff's conclusions regarding SolarWinds' failure to consistently follow the cybersecurity practices in their Security Statement into his methodology, their arguments still fail. Mr. Graff explained in extensive detail what he meant when he said that SolarWinds' "internal documents indicate that SolarWinds failed to consistently apply" the relevant cybersecurity practices. Graff Rep. ¶ 48.

For example, with respect to access controls, Mr. Graff opines that "the practices SolarWinds described in internal documents were inconsistent, from a cybersecurity perspective, with certain access control related assertions made in the Security Statement." *Id*. ¶ 52. Specifically, he explains, "that SolarWinds was internally aware of significant access control problems that substantially raised the company's cybersecurity risk profile." *Id*. He describes specific examples in which SolarWinds' internal documents indicated that the company's practices did not consistently conform to the Security Statement's access control representations:

- Paragraphs 61-66 analyze internal assessments regarding the concept of "least privilege" not being followed or audited and "inappropriate" access and privilege being granted.
- Paragraphs 67-74 evaluate a 2019 assessment regarding SolarWinds' Managed Service Provider (MSP) line of business in which MSP support staff had been given an "excessive" level of access to both MSPs and MSP customers.
- Paragraphs 75-93 analyze two incidents, one in which Super User access was inappropriately granted, and another in which a password to a sensitive system was made publicly available, in conjunction with multiple internal presentations describing systemic issues with regards to identity management and access controls
- Paragraphs 94-99 analyze internal presentations and emails regarding employees leaving the company and potentially retaining access to critical systems and providing a system access request form ("SARF") that illustrated this concern. After going through these specific examples described in the company's own internal documents, in paragraphs 100-110, Mr. Graff explained and opined on the significance of such failures with respect to access controls and how they deviated from the representations in the Security Statement: "In the aggregate, the wide range of access control failures I described in the preceding sections not only constituted a departure from the assertions in the Security Statement, but also exposed both SolarWinds and its customers to elevated cybersecurity risks."

Thus, if Defendants had any doubt as to the basis for Mr. Graff's conclusion that SolarWinds did not consistently follow the representations in the Security Statement regarding access controls, or what he meant by that, they need only have read his report to divine it. The same holds true for each of the subsequent sections of his report concerning passwords and user authentication (*id*. ¶¶ 111-136) and the software development lifecycle (*id*. ¶¶ 137-190).

Defendants' citation to cases in which experts made "assertions without explaining the basis for the assertions" or "fail[ed] to define" technical jargon are thus inapposite. *See* Def. Mot. at 16 (citing *SEC v. Lek Sec. Corp.*, 370 F. Supp. 3d 384, 416 (S.D.N.Y. 2019)). Likewise, Defendants' reliance on a case in which this Court excluded an expert who failed to properly support his conclusion is unavailing. *See id*. (citing *LVL XIII Brands, Inc. v. Louis Vuitton Malletier S.A.*, 209 F. Supp. 3d 612, 647 (S.D.N.Y. 2016), *aff'd*, 720 F. App'x 24 (2d Cir. 2017)) (Engelmayer, J.). In that case, the Court distinguished the expert before it from a different expert who "did not leave the court to speculate how his review of those sources ultimately led to his conclusion" and who described the criteria "derived from his professional experience, academic studies, and other documents that he used when formulating his opinions." *LVL XIII Brands, Inc.*, 209 F. Supp. 3d at 647 (cleaned up). That is precisely what Mr. Graff has done in his report.

B. Defendants' Attempts to Challenge the Substance of Mr. Graff's Opinions are Wholly Improper in a *Daubert* Motion.

Defendants devote seven pages of their motion to arguing that the serious cybersecurity failures that Mr. Graff identified at SolarWinds are not really as serious as he says. *See* Def. Mot. at 16-22. Similar to their quibbling with the word "consistently" (discussed above), they nitpick Mr. Graff's *conclusion* that certain cybersecurity failures at SolarWinds were of such magnitude that they were indicative of "systemic" problems. *Id*. at 16-18. Once again, they try to "package[] in *Daubert* terms" what "is in substance a disagreement with [the expert's] conclusions." *In re*

Aluminum Warehousing Antitrust Litig., 336 F.R.D. at 34. Even if there were any merit to Defendants' substantive challenges (which the SEC disputes), the Supreme Court has made clear that "[v]igorous cross-examination, presentation of contrary evidence, and careful instruction on the burden of proof are the traditional and appropriate means of attacking shaky but admissible evidence." *Daubert*, 509 U.S. at 596. If Defendants are confident that Mr. Graff's opinions will not withstand scrutiny, they will have their opportunity to cross-examine him at trial. But, trying to hide his opinions from the jury because they disagree with them is antithetical to our adversary system. *See In re Joint E. & S. Dist. Asbestos Litig.*, 52 F.3d 1124, 1135 (2d Cir. 1995) ("Trial courts should not arrogate the jury's role in evaluating the evidence and the credibility of expert witnesses by simply choosing sides in the battle of the experts.") (cleaned up); *see also In re LIBOR-Based Fin. Instruments Antitrust Litig*., 299 F. Supp. 3d 430, 471 (S.D.N.Y. 2018) ("A *Daubert* motion is an improper venue in which to take sides in a battle of the experts offered by competing parties.") (cleaned up).

Despite this clear authority, Defendants ask this Court to decide that Mr. Graff was wrong when, based on his decades of cybersecurity experience and reference to well-accepted industry guidance, he determined that the SolarWinds cybersecurity problems contemporaneously noted by its employees represented serious cybersecurity failures that deviated from the public representations in the Security Statement. They even ask the Court to not only rule on a motion that the SEC's expert is wrong, but that their own expert, Dr. Rattray *is right*. *See e.g.*, Def. Mot. at 18-20 (highlighting dispute between Mr. Graff and Dr. Rattray over the severity of "SuperUser" being given to developers who did not need such access). They go so far as to block quote an argument from Dr. Rattray's report in which he employs a strained

analogy to a file cabinet and spilled coffee. *See id*. at 19-20.[9] Instead of relying on a questionable analogy, Mr. Graff explained in detail in his report the problems associated with such inappropriate access and cited industry bodies, such as NIST and ISO to support his conclusion (*see* Graff Rep. ¶¶ 81-85, 151-162), as to why this was "indicative of systemic issues at SolarWinds." *Id*. ¶ 157.[10]

Defendants continue in this vein when they challenge Mr. Graff's opinions regarding several other incidents. *See* Def. Mot. at 20-21. Specifically, they argue with his conclusions regarding MSP customer support being granted inappropriate access. *Id*. Yet, Mr. Graff explained in detail, citing NIST and other industry bodies, why he concluded that this was a potentially catastrophic problem. *See* Graff Rep. ¶¶ 70-73 ("Providing 'system level access' […] to people who do not need it is a serious access control issue and a violation of the least privilege

[9] Even worse is Defendants' reliance on their expert's flawed analogy regarding Aaron Judge. Def. Mot. at 17. Their expert gets the basic facts of his own analogy wrong by claiming that Judge "cost the Yankees the final game." In fact, the Yankees still led 5-0 in the fifth inning after Judge's error, and despite a series of errors and misplays that followed in the top of the inning, the game was still tied after the third out. The Yankees took the lead again in the sixth inning but later gave up two more runs to the Dodgers in the eighth inning, partly attributable to a catcher's interference call (an error) against them. Putting aside the reasonableness of any company comparing itself to the 27-time champion Bronx Bombers, it is ironic that Defendants use an analogy where, in truth a collective breakdown in defense led to a significant loss to argue that their own failures were not systemic. Moreover, these types of disagreements between experts over the systemic nature of a problem are not appropriately resolved in a *Daubert* motion. *See In re LIBOR-Based Fin. Instruments Antitrust Litig.*, 299 F. Supp. 3d at 471.

[10] Not only is it inappropriate for Defendants to challenge Mr. Graff's substantive conclusions in a *Daubert* motion, as discussed more thoroughly in the SEC's response to Defendants' summary judgment motion in which they make the same semantic argument about the meaning of "systemic," Defendants are just plain wrong in their critique. As Mr. Graff explained in his Opening Report, based on the fundamental cybersecurity principle "defense-in-depth," the system should be set up in a way to "apply multiple security layers to ensure that vulnerabilities not remediated by one countermeasure are addressed by another." (*see* Graff Rep. ¶ 35 a.). In other words, the very fact that one person's actions can create such substantial security risks without checks and balances in place is, in and of itself, a systemic issue. Rather than an individual failure, the lack of appropriate controls is a systemic weakness.

principle, an important element of access control best practice."). They also argue with his opinion regarding the severity of the password "solarwinds123" being publicly leaked and the potential for it to be used to disseminate malicious code to customers. Def. Mot. at 21. Again, Mr. Graff cited industry bodies such as OWASP, NIST, and ISO, as well as chapter from a cybersecurity reference book *that he co-authored*, to explain why this was a serious cybersecurity problem. *See* Graff Rep. ¶¶ 126-127, 130-131 ("One commonly accepted industry norm is that storing plaintext or hard-coded passwords in configuration files violates best practices."). Defendants even argue in their motion, based on a declaration they submitted in conjunction with their summary judgment motion (from a witness not disclosed during discovery), that "the account could not have been used to replace SolarWinds files with malicious files on SolarWinds download site." Def. Mot. at 21 & n. 18.

These are precisely the type of substantive disputes that are not properly raised in a *Daubert* challenge. *See SEC v. Ripple Labs, Inc.,* 2023 WL 5670711, at *11 (S.D.N.Y. Mar. 6, 2023) ("Defendants may challenge [the expert's] opinion at trial on the ground that he ignored relevant factors or misapplied the factors he did consider, but disagreement over an expert's conclusions does not warrant exclusion."). Defendants are free to raise all these points with Mr. Graff when they cross-examine him at trial, but the Court should reject considering them now and leave that consideration for the jury.[11]

[11] Defendants make a perplexing argument about how Mr. Graff gave testimony before Congress while the CISO at NASDAQ that was somehow at odds with his opinions in this case. *See* Def. Mot. at 23-25. As Mr. Graff explained several times at his deposition, the failover controls at issue in the so-called "Flash Freeze" could not even remotely be considered cybersecurity controls and thus were not even under his purview as the CISO. *See e.g.*, Graff Depo. at 87:2-7, 96:15-97:8 ("[T]his wasn't a cybersecurity incident by any stretch of the imagination. . . .") (Exhibit B). In any event, "as with any witness, inconsistencies in an expert witness's testimony do not implicate *Daubert*, but rather are properly addressed during cross examination." *In re Fosamax Prods. Liab. Litig.*, 924 F. Supp. 2d 477, 496 (S.D.N.Y. 2013).

V. Mr. Graff is not Opining on Scienter.

Defendants conclude their motion with a perfunctory argument that alleges that Mr. Graff is opining on Defendants' state of mind "in an attempt to shore up the SEC's scienter allegations." Def. Mot. at 25. Mr. Graff does no such thing. Indeed, the only two examples that Defendants point to demonstrate that he is not offering any opinions about state of mind.

First, Defendants quote from his opening report where he stated: "The fact that such simple issues slipped through the company's internal systems should have alerted SolarWinds' cybersecurity leadership of potential systemic issues." *Id*. (quoting Graff Rep. ¶ 28). In that paragraph Mr. Graff was not opining about what specific employees knew. Instead, as is evident from the context of the paragraph, Mr. Graff was offering a technical cybersecurity opinion that *if senior cybersecurity executives were not aware* of the company violating such elementary cybersecurity principles, then this lack of knowledge, in and of itself, indicates a systemic problem at the company. Indeed, the two sentences that preceded the one quoted by Defendants make that clear. *See* Graff Rep. ¶ 28 ("Many of the cybersecurity norms that SolarWinds violated were elementary in nature, part of the fundamental blocking and tackling that constitutes everyday cybersecurity. For example, the need to separate production and development environments is so fundamental that I teach this to my students as part of my introductory undergraduate System Security class.").

Second, Defendants quote from Mr. Graff's rebuttal report where he "also concluded that significant deficiencies within these areas were known or made known to the relevant cybersecurity and leadership personnel" and "should have alerted SolarWinds' cybersecurity leadership that the Security Statement was inaccurately describing SolarWinds' cybersecurity posture." Def. Mot. at 25 (quoting Graff Rebuttal ¶ 2). The first phrase is not an opinion by Mr. Graff. Instead, it is him stating that the factual record shows that incidents that he discusses in his

report were made known to those at SolarWinds who oversaw cybersecurity. This is entirely proper for an expert witness. *See CFTC v. Wilson*, 2016 WL 7229056, at *8 (S.D.N.Y. Sept. 30, 2016) ("An expert can also reference an actor's state of mind when that state of mind is in the record and is the basis for the expert's ultimate opinion.") (cleaned up). Indeed, Defendants do not dispute that company leadership knew of these incidents—they spend a large part of their summary judgment brief attempting to explain away the significance of those incidents by pointing to deposition testimony and declarations from those employees. *See e.g.*, Def. Mot. for SJ at 25-31 (relying on deposition testimony and declarations from various witnesses to contest the meaning of company documents).

The second part of the statement—that these facts "should have alerted SolarWinds' cybersecurity leadership that the Security Statement was inaccurately describing SolarWinds' cybersecurity posture" (Def. Mot. at 25 (quoting Graff Rebuttal ¶ 2))—is Mr. Graff expressing the technical expert opinion that the facts indisputably known to SolarWinds' cybersecurity leadership *should have* alerted them to the discrepancy between the practices and the representations in the Security Statement. He is not opining on their actual state of mind but "what an action may indicate about a party's state of mind." *Wilson*, 2016 WL 7229056, at *8. Expert opinions of this nature are not only acceptable but routine in federal courts. *See id*. ("[A]n expert can testify to whether a given practice is consistent with a given state of mind."). The Court should thus reject Defendants' mischaracterization of Mr. Graff's opinions.

CONCLUSION

For the foregoing reasons, the Commission respectfully requests that the Court deny Defendants' motion.

Dated: June 13, 2025

Respectfully submitted,

/s/ John J. Todor

John J. Todor
(admitted *pro hac vice*)
Christopher M. Bruckmann
(SDNY Bar No. CB-7317)
Christopher J. Carney
Kristen M. Warden
(admitted *pro hac vice*)
William B. Ney
(admitted *pro hac vice*)
Benjamin Brutlag
(SDNY Bar No. BB-1196)
Lory Stone
(admitted *pro hac vice*)
Securities and Exchange Commission
100 F Street, NE
Washington, D.C. 20549
202-551-5381 (Todor)
202-551-5986 (Bruckmann)
202-551-2379 (Carney)
202-551-4661 (Warden)
202-551-5317 (Ney)
202-551-2421 (Brutlag)
202-551-4931 (Stone)
TodorJ@sec.gov
BruckmannC@sec.gov
Carneyc@sec.gov
WardenK@sec.gov
NeyW@sec.gov
BrutlagB@sec.gov
StoneL@sec.gov

Attorneys for Plaintiff
Securities and Exchange Commission